

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA,
Plaintiff,

Case No. 3:17-CR-00216-AA
OPINION AND ORDER

vs.
LELAND TODD BOOZER
Defendant.

AIKEN, District Judge:

On June 13, 2017, defendant Leland Todd Boozer was indicted on two counts of distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (b)(1), and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). On March 5, 2018, defendant filed a motion to suppress, request for production of witness statements, or, in the alternative, motion for a *Franks* hearing. For the reasons set forth herein, the Court grants the motion to

suppress, denies without prejudice at this time the request for production of witness statements,¹ and denies the motion for a *Franks* hearing.

BACKGROUND

On September 16, 2012, U.S. Secret Service Special Agent David Huntoon performed an internet investigation for the identification of individuals who possess and share child pornography on the Ares network a Peer to Peer (“P2P”) file sharing program. In his search, Agent Huntoon found a computer, with the IP address 76.105.250.200, willing to share 52 files on the Ares network. Agent Huntoon downloaded seven of the fifty-two files from that IP address. The files were *files of interest*, meaning the files had been previously identified by law enforcement as pertaining to the exploitation of children. Law enforcement agencies use software to identify files of interest that have been previously identified by law enforcement as pertaining to child exploitation by their hash value, an alpha-numeric value generated to serve as a file’s digital finger print.² A file becomes a file of interest when the hash value has been previously identified by law enforcement as one that

¹ Rule 26.2 for the Federal Rules of Criminal Procedure states that “[a]fter a witness other than the defendant has testified on direct examination, the court, on motion of a party who did not call the witness, must order an attorney for the government . . . to produce, for the examination and use of the moving party, any statement of the witness that is in their possession and that relates to the subject matter of the witness’s testimony. In their response motion, “[t]he government has already produced all written reports, logs, and similar documents pertaining to the undercover downloads.” Doc. 31 at 2. Additionally, the government states that “[m]ost of the witnesses who the government expects to call at the suppression hearing did not testify before the grand jury.” Doc. 31 at 2. Absent of identification of specific information, this Court must deny the motion.

² The software then logs the IP address of a computer offering to share files of interest and attempts to download those files from the computer.

could have child pornography, depicted subjects that may or may not be under 18, child erotica, or non-pornographic images from a known child pornography series. Agent Huntoon sent the hash values of the downloaded files to the National Center for Missing and Exploited Children (“NCMEC”). NCMEC reported to Agent Huntoon that one of the files submitted had not been previously submitted to NCMEC, one file depicted a child victim who had been previously identified by a law enforcement officer, and six files had been previously submitted to the NCMEC, but the children and had not been positively identified.

On September 19, 2012, Agent Huntoon sent U.S. Secret Service Special Agent Adam Sale the downloaded files, hash values, and IP address information. Agent Sale determined on September 21, 2012 that Comcast, an internet provider, assigned the IP address in question. Five days later, on September 27, 2012, Agent Sale sent a summons to Comcast for the information regarding the identity of the subscriber to the IP address. Comcast responded that defendant, Leland Boozer, was the subscriber and that the address on the account was 3761 SE Division St., Portland OR, 97402-1547. The U.S. Postal service confirmed that the address in question was listed under defendant’s name. In November 2012, Assistant U.S. Attorney (“AUSA”) Gary Sussman requested Agent Sale draft an affidavit in support of a search warrant to search Boozer’s residence. After the draft was submitted in December 2012, the AUSA requested additional investigation.

In March 2013, Agent Sale contacted AUSA Sussman about the search warrant for Boozer’s address; AUSA Sussman requested that another attempt be

made to download files from Boozer's IP address to freshen the probable cause for the search warrant. Agent Sale reported that Agent Huntoon was not able to complete any additional downloads, and the IP address in question was no longer logged into the Ares network. The following June, Agent Sale asked AUSA Sussman request a subpoena for defendant's IP address, and AUSA Sussman asked Agent Sale to pursue other options before seeking the subpoena. Agent Sale also consulted with Special Agent Jim Williams of the Oregon Internet Crimes Against Children Task Force ("ICAC") about other investigative options. Agents Sale submitted another draft warrant the AUSA in July of 2013, but the warrant was not presented to a Magistrate Judge at that time.

On October 31, 2013, Agent Sale, Agent Williams, and ICAC Special Agent Mark Posler went to defendant's address to do a "knock and talk" – a consensual encounter in which they hoped to talk to defendant about the investigation. Agents arrived at the residence between 9:00 am and 10:30 am. Defendant was not home, but his roommate Camelia Nine was home and answered the door. The agents identified themselves to Ms. Nine and explained that they were investigating the downloading of computer files by someone in the apartment complex. Ms. Nine gave the agents verbal consent to enter the apartment. Once inside, the agents saw a computer system set up and operating in the living room. Ms. Nine explained that the computer in the living room belonged to defendant, and that she owned an Apple computer. Ms. Nine also stated that defendant had the computer built about five months previously. Ms. Nine consented to a search of her computer. In front of

Ms. Nine, Agent Posler told Agent Sale that there was no evidence of child pornography or Ares client software on the computer. After some further discussion, the agents left the apartment and asked Ms. Nine not to contact defendant.

After leaving the apartment, Agent Sale drove to defendant's workplace while Agent Posler and Williams waited in a separate car near his apartment. Once Agent Sale arrived at defendant's place of work, he spoke with the human resources director. The director informed him that defendant left about half an hour previously to go home. Agent Sale was unable to locate defendant at or around his workplace. Agent Sale returned to defendant's apartment, and Ms. Nine again invited the agents into the apartment. Ms. Nine stated that she called defendant after the agents left and told him that the agents had come to the apartment and were looking for computers with the Ares P2P file sharing program. Ms. Nine allowed the agents to remain in the apartment waiting for defendant to return home. She also phoned defendant again and asked him to return home to speak with the agents. Defendant never returned to the apartment while the agents waited for him to return. Agent Sale stated that he grew concerned about the possibility of defendant returning home and destroying the evidence stored on his computer. Thus, at around 12:30 pm, after consulting with a prosecutor, Agent Sale seized the computer until he could apply for a search warrant.

After Agent Sale seized the computer, Agent Posler helped in disconnecting the computer and all the equipment. During this process, Agent Sale reported that

the side panel of the computer tower fell off as it was pulled from under a table, which exposed the contents of the tower. Agent Sale and Agent Posler saw into the computer tower and noted one hard drive mounted into the computer tower and two additional hard drives sitting on the bottom of the tower. These other two hard drives were dusty and appeared to the agents to be older than five months. Agent Posler then arranged the tower and the additional hard drives inside to be transported without being damaged. Agent Sale took possession of all the computer equipment.

Eight days later, on November 8, 2013, Agent Sale presented an affidavit for a search warrant to U.S. Magistrate Judge Paul Papak who granted a warrant to search the contents of the items seized from defendant's apartment.³ Prior to the issuance of the warrant, Agent Posler secured the computer equipment in his forensic laboratory without searching or examining it.

Agent Sale sent copies of the warrant, the application, and the affidavit to Agent Posler informing him that the task force could proceed with the examination. Agent Sale neglected, however, to send Attachments A and B of the warrant to Agent Posler. Attachment A described the items that were to be searched, while Attachment B described the items that could be searched for and seized and when the search had to be completed. The time limit was 180 days. Agent Posler noticed Attachment A was missing from the documents he received from Agent Sale. After

³ In his declaration, Agent Sale notes that he drafted the affidavit two days after the search, and then sent it U.S. Attorney for review. Revisions and edits were then traded over the next few days before the final affidavit was submitted to Magistrate Judge Papak.

inquiring, Agent Sale sent Attachment A to him. Agent Posler never received Attachment B, but he avers that he knew the warrant authorized a search for evidence of child pornography offenses. Agent Posler began imaging the first of the devices on November 12, 2013, and all the forensic images were completed and verified by November 21, 2013. Agent Sale then retrieved the computer equipment on December 3, 2013 and returned it to the Secret Service's evidence vault. The initial forensic examination of the computer equipment was completed on or about June 1, 2016, some two and a half years later. On June 13, 2017, defendant was indicted on child pornography charges. Doc. 1.

On November 28, 2017, Secret Service Special Agent Carl Klein obtained a second search warrant from U.S. Magistrate Judge Paul Papak for the computer equipment. The second warrant was to cure deficiencies of the previous warrant regarding Attachment A and B and the fact that a return that was never filed. In his affidavit in support of the warrant, Agent Klein attested that the images taken during the initial examination would be sealed and a new examination would be conducted by a new examiner. After the warrant was issued, Agent Klein took the computer equipment to the United States Department of Homeland Security forensic laboratory in Portland.

On December 11, 2017, after the re-examination of the computer began, defendant filed a motion for a stay in the examination and requested a discovery and evidentiary hearing. This Court denied that motion. Doc. 17.

On March 5, 2018, defendant filed the present motion to suppress, request for production of witness statements, and, in the alternative, motion for a *Franks* hearing. Doc. 24. An evidentiary hearing was held October 22, 2018. Doc. 45. Following the hearings, the parties engaged in supplemental briefing to the Court.

STANDARD OF REVIEW

The Fourth Amendment prohibits unreasonable searches and seizures by the government. U.S. Const. Amend. IV. In the context of personal property, and particularly containers, the Fourth Amendment challenge is typically to the subsequent search of the container rather than to its initial seizure by the authorities. *United States v. Place*, 462 U.S. 696, 700–01, (1983). In the ordinary case, seizure of personal property is *per se* unreasonable within the meaning of the Fourth Amendment unless it is accomplished pursuant to a judicial warrant issued upon probable cause and particularly describing the items to be seized. *Id.* Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Supreme Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present. *Id.*

A warrantless seizure requires both probable cause and exigent circumstances. Probable cause exists when “there is a fair probability that contraband or evidence of a crime will be found in particular place.” *Illinois v.*

Gates, 462 U.S. 213, 238 (1983). Further describing that probable cause is “a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.” *Id.* at 232. The Ninth Circuit has defined exigent circumstances as those that “would cause a reasonable person to believe that [a seizure] . . . was necessary to prevent physical harm to the officers or other person, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.” *United States v. Brooks*, 367 F.3d 1128, 1135 (9th Cir. 2004) (internal quotation marks and citation omitted). Exigent circumstances are fact specific and depend on the totality of the circumstances. *United States v. Arellano-Ochoa*, 461 F.3d 1142, 1145 (9th Cir. 2006). The exigencies must be viewed from the totality of circumstances known to the officers at the time of the warrantless intrusion. *United States v. Licata*, 761 F.2d 537, 543 (9th Cir. 1985) (citing *People of Territory of Guam v. Borja*, 732 F.2d 733, 736 (9th Cir. 1984)).

“Evidence derivative of a Fourth Amendment violation—the so-called fruit of the poisonous tree—is ordinarily tainted by the prior illegality and thus inadmissible, subject to a few recognized exceptions.” *United States v. Gorman*, 859 F.3d 706, 716 (9th Cir. 2017) (internal citations and quotation marks omitted). As a general rule, the defendant bears the burden of proof on a motion to suppress evidence. *United States v. Caymen*, 404 F.3d 1196, 1199 (9th Cir. 2005). Because warrantless searches are presumptively unreasonable, however, the burden of

proving that a warrantless seizure did not violate the Fourth Amendment is on the government. *United States v. Scott*, 705 F.3d 410, 416 (9th Cir. 2012).

Not every violation of the Fourth Amendment triggers the application of the exclusionary rule. *Herring v. United States*, 555 U.S. 135, 140 (2009) (the fact that a Fourth Amendment violation occurs “does not necessarily mean that the exclusionary rule applies;” the Supreme Court has “repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation”). The exclusionary rule’s “sole purpose” is “to deter future Fourth Amendment violations.” *Davis v. United States*, 564 U.S. 229, 236-37 (2011). A court must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.⁴ *Place*, 462 U.S. at 703. When the nature and extent of the detention are minimally intrusive of the individual's Fourth Amendment interests, the opposing law enforcement interests can support a seizure based on less than probable cause. *Id.*

///

///

///

⁴ “Different interests are implicated by a seizure than by a search.” *Segura v. United States*, 468 U.S. 796, 806 (1984). A seizure “affects only the person’s possessory interests,” whereas a search “affects a person’s privacy interests.” *Id.* at 806. Society’s interest in “the discovery and protection of incriminating evidence from removal or destruction can supersede, at least for a limited time period, a person’s possessory interest in property, provided that there is probable cause to believe that [the] property is associated with criminal activity.” *Id.* at 808.

DISCUSSION

I. *Motion to Suppress*

This Court finds that the seizure of defendant's computer violated defendant rights under the Fourth Amendment of the Constitution, as there were no exigent circumstances and probable cause was too stale to justify the warrantless seizure.⁵

A. *Warrantless Seizure of the Home Computer*

Defendant argues that there was no probable cause or exigent circumstance to justify the warrantless seizure of his computer and hard drives, and therefore, the exclusionary rule requires suppression of this evidence. Defendant maintains that probable cause for the seizure and subsequent search was stale. Defendant further contends that there was no exigency that would allow the government to seize his computer during the October 31, 2013 knock and talk.

1. *Probable Cause to Seize the Computer*

Defendant argues that the probable cause upon which the warrantless seizure was based was stale due to the thirteen-month intervening period between Agent Huntoon downloading files from defendants' IP address and the October 31, 2013 warrantless seizure. To seize by exigency, both probable cause and exigency must exist. Specifically, a container can be seized without a warrant if an officer has “[p]robable cause to believe that [it] holds contraband or evidence of a crime ... pending issuance of a warrant to examine its contents, if the exigencies of the

⁵ As the Court finds find there were no exigent circumstances and no probable cause, there is no need to analyze defendant's arguments regarding the hard drives found in his computer tower.

circumstances demand it or some other recognized exception to the warrant requirement is present.” *Place*, 462 U.S. at 701. A staleness claim must be evaluated by this Court “[i]n light of the particular facts of the case and the nature of the criminal activity and property sought.” *United States v. Greathouse*, 297 F. Supp. 2d 1264, 1270 (D. Or. 2003). “[T]he mere lapse of substantial amounts of time is not controlling.” *Greathouse*, 297 F. Supp. 2d at 1270 (quoting *Lacy*, 119 F.3d at 745). Probable cause is not stale “if there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises.” *United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (quoting *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997)).

Defendant argues that the thirteen-month lapse in time from the initial download to when the computer was seized alone caused the probable cause in this case to become stale. Defendant also argues that there was an intervening event that further diminishes probable cause. The computer in question was built eight months after the initial download and five months prior to when the agents seized it. Importantly, the agents were made aware of this fact when initially interviewing Ms. Nine. Defendant argues that once the agents knew that the computer was purchased after the date Agent Huntoon download the illicit files, they did not have probable cause to believe that those files were on this new computer.

The government argues that there was enough probable cause to believe that evidence of the crimes of distribution and possession of child pornography would be found on defendant’s computer equipment for several reasons. First, less than

fourteen months before the knock and talk, Agent Huntoon had downloaded child pornography files from an IP address known associated with defendant and his home address. When agents questioned Ms. Nine, she revealed that both she and defendant accessed the internet through a secure wireless network which required a password to access. However, she also told agents that to her knowledge no one other than defendant and herself had access to the network and used it. Finally, the government argues that once agents searched Ms. Nine's personal computer and found no evidence of child pornography or the Ares P2P software, Agent Sale had probable cause to believe that evidence of the crimes of distribution and possession of child pornography would be found on defendant's computer equipment. As to defendant's argument that Ms. Nine revealed that the computer in question was built several months after September 2012 downloads by Agent Huntoon, the government responds that agents saw the two older hard drives which looked as though they had been salvaged from an older computer after the panel came off of the tower.

Information is not stale if "there is a sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." *Lacy*, 119 F.3d at 745. See also *Schesso*, 730 F.3d 1040 (panel held that the issuing judge had ample reason to believe that child pornography uploaded to peer to peer file sharing network would be present at the defendants residence twenty months after the upload, where the affiant explained that individuals who possess, distribute, or trade in child pornography, "rarely, if ever, dispose of

sexually explicit images of children because these images are treated as prized possessions.”)

The government urges that here, as in *Schesso*, Agent Sale knew and attested, based on his training and experience, that “individuals who collect and trade in child pornography” often retain their collections of child pornography “for extended periods of time,” and “treat their collections as prized possessions, rarely disposing of them entirely.” Ex. A at 52, ¶ 16. Thus, the fourteen-month delay here did not alone mean the necessary probable cause had become stale.

The Court finds that probable cause was too stale here to justify the seizure. Prior to the knock and talk, agents were told by prosecutors that more investigatory work needed to be done to freshen probable cause. Then upon engaging with defendant’s roommate thirteen months after the initial downloads, agents learned that the computer system belonging to defendant was only approximately five months old. The government also could not explain the existence of a third computer in the apartment which appeared much older than tower which was seized. Ex. E3. Agents testified that they know nothing about that computer. No questions were asked of Ms. Nine about it. Nothing was done about it save, taking photos. The Government argues that the existence of this tower is not relevant, however, at a minimum it would certainly fail to enhance probable cause to support a seizure of the newer computer tower. Finally, the government’s argument regarding the two older hard drives found in the computer tower, overlooks the fact that agents only learned of them after beginning a warrantless seizure.

The Court is mindful that probable cause must be judged on the particular facts of this case. While this case presents a close question, the Court finds that agents did not have sufficient probable cause seizure of the computer tower. While it is true that in a number of child pornography cases staleness arguments based on the passage of time alone have been rejected by other courts, it is still an important factor to be considered. Given the thirteen months between obtaining the initial evidence and the October 2013 seizure, defendant's lack of prior criminal history or contact with law enforcement, the lack of evidence regarding ongoing criminal activity, as well as the agents knowledge that computer in question was built well after Agent Huntoon's downloads, the Court finds that the information giving rise to probable cause was too stale at the time of the warrantless seizure to justify the government's actions.

2. *Exigent Circumstances*

As the Court noted, the question of whether probable cause was stale at the time of the seizure is a close question. However, even assuming that there was probable cause to believe evidence of the alleged criminal activity would be found on the computer, the Court finds that there were no exigent circumstances which justified the warrantless seizure, and the government had ample opportunity to seek a warrant from a Magistrate Judge at the time of the seizure.

Exigent circumstances are those that "would cause a reasonable person to believe that [a seizure] . . . was necessary to prevent physical harm to the officers or other person, the destruction of relevant evidence, the escape of the suspect, or some

other consequence improperly frustrating legitimate law enforcement efforts.” *Brooks*, 367 F.3d at 1135 (internal quotation marks and citation omitted). Here, the government maintains that exigency existed because the agents justifiably believed that the seizure was necessary to prevent the destruction of evidence, namely the contraband files they believed were contained on defendants’ computer.

Defendant urges that his actions did not rise to the level of exigency required to justify a warrantless search. After defendant learned that agents had spoken with Ms. Nine, he did not return home and could not be located at work. Agent Sale stated that he thought defendant was trying to avoid them. Further, Agent Sale explained that did not think that securing the computer equipment at the defendant’s residence while he applied for a warrant was a good option at that point.

Inconvenience does not give rise to an exigent circumstance. *See Coolidge v. New Hampshire*, 403 U.S. 443, 469 (1971) (without actual objective evidence of exigency, inconvenience in procuring a warrant is insufficient to justify warrantless seizure). When an officer claims that securing a warrant is impractical there must be objective facts demonstrating exigency over the mere refusal to comply with an officer’s request. *Missouri v. McNelly*, 569 U.S. 141, 146 (2013). Defendant states that the government hasn’t put forward any argument explaining why obtaining a warrant was unavailable or impractical. *United States v. Alvarez*, 810 F.2d 879, 883 (9th Cir. 1987).

The government argues that the failure to obtain a warrant for computer was not based on inconvenience to the agents. Rather, the government notes that the agents were in the middle of an investigation for much of the time that defendant contends they could have sought a warrant. Part of the two hours spent investigating on October 31, 2013, were taken up with Agent Sale traveling to and from defendant's place of work. Another portion of that time was used to converse with Ms. Nine and look at her computer. The government contends that it would have been impractical and that it was not required of Agent Sale to stop and get a search warrant at the first hint of probable cause, particularly since defendant appeared to be avoiding the agents, and electronic data can be easily destroyed.

Defendant cites to *Kentucky v. King*, arguing that the agents created the exigency to seize the computer. 131 S. Ct. 1849, 1862 (2011). However, the Court there held that "the exigent circumstances rule applies when the police do not gain entry to premises by means of an actual or threatened violations of the Fourth Amendment." *Id.* The government correctly points out that Ms. Nine consented to the officers entering the apartment. Still, defendant seeks to distinguish *King*.⁶ There, the Supreme Court found no violation of the Fourth Amendment based on the police-created exigency doctrine where officers knocked on a door and then heard noises coming from the apartment which officers believed consistent with noise in the destruction of evidence before immediately entering the premises

⁶ Defendant also seeks to distinguish similar cases where a warrantless seizure was upheld. See *United States v. Brown*, 701 F.3d 120 (9th Cir. 2012); *United States v. Licata*, 761 F.2d 537, 543 (9th Cir. 1985)

without a warrant. Defendant contrasts the facts in this case arguing that agents relied on subjective speculation about what might or might not have happened. Here defendant notes that he was at work during the seizure while the agents knew that computer was secure in his apartment. Defendant argues that it would have been easier to secure the computer and pursue an electronic warrant while defendant avoided contact with the agents that were in his apartment.

In *King*, the Supreme Court approvingly noted that “the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment,” *Mincey v. Arizona*, 437 U.S. 385, 394 (1978). Defendant argues that these circumstances are “distinct from one where law enforcement must act with exigency ‘to prevent the imminent destruction of evidence.’” *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

The government argues that the exigency was not speculative nor did the agents create it. Once Ms. Nine called defendant to inform him about the agents’ presence in the home and that they were looking for child pornography, the agents reasonably inferred that defendant was avoiding contact with them due his sudden departure from his work. Defendant told her that he would return home, but he did not do so prior to the seizure of the computer. Instead, later defendant told her that he was still at work despite Agent Sale being unable to locate him there. The government further argues that defendant “had every incentive to delete or destroy the evidence on his computer equipment.” See *United States v. Licata*, 761 F.2d 537, 543 (9th Cir. 1985) (noted that evidence stored on a computer is fragile and that in

the totality of the circumstances that the officers knew at the time exigency existed for the officers to seize the computer.) Given “[t]he fragile and easily destructible nature of digital evidence at issue” the government argues that the agents had “undeniable concerns regarding loss or possible destruction of contraband by the owner.”⁷ *United States v. Blood*, 429 Fed. Appx. 670, 671 (9th Cir. 2011)

The government contends that if the agents left to seek a warrant the defendant or Ms. Nine, at defendant’s direction, could have easily deleted the files in question. Further, if they secured the residence, as defendant suggests, the agents, one of whom was a computer forensics expert, would have to deal with the defendant and Ms. Nine while trying to secure computer equipment, which would have raised officer safety concerns. Thus, the government argues that the Agent Sale had ample reason to seize the computer until he could apply for a warrant to search it.

The government also cites to several exemplary cases where the court found exigent circumstances for a warrantless seizure. For example, the Ninth Circuit in *Blood* reversed a district court’s order suppressing evidence where federal agents had probable cause to believe that the defendant’s laptop computer contained child pornography, and where the defendant admitted deleting child pornography files

⁷ See also *United States v. Brown*, 701 F.3d 120, 127 (4th Cir. 2012) (held that it was reasonable for detectives to seize the defendant’s computer “to prevent the destruction of relevant evidence” where the defendant knew they were investigating “internet crimes against children.”); *United States v. Bradley*, 488 Fed. Appx. 99, 103 (6th Cir. 2012) (“[c]ourts have doubted the wisdom of leaving the owner of easily-destructible contraband in possession of that contraband once the owner is aware that law-enforcement agents are seeking a search warrant.”)

from his computer in the past “because he knew them to be illegal.”⁸ *Id.* However, there, the defendant admitted to possessing contraband and the suspected laptop computer was in the suspect’s physical possession during a face-to-face encounter with law enforcement. During the encounter, the suspect also admitted to previously deleting contraband files on his computer and, at the end of the consensual interview, the agents seized the computer based on exigency. The immediacy of Mr. Blood’s control over and custody of the computer is in stark contrast to the facts here.

What distinguishes this case from *Blood* and others cited by the government is that there was no imminent threat that the evidence in question would be destroyed or that defendant had possession of the evidence in question. Defendant may have had incentive to destroy evidence, though there is no evidence he had done so in the past or was planning to do so. More importantly, there is no firm evidence that he any opportunity to act upon that supposed incentive. Defendant

⁸ See also *United States v. Betché*, 540 Fed. Appx. 838, 843 (10th Cir. 2013) (upheld a warrantless seizure of computer where agents had probable cause to believe it contained child pornography in which the officers had “reason to believe that [he] might destroy the evidence,” and “no police manipulation created the exigency.”); *United States v. Bradley*, 488 Fed. Appx. 99, 103 (6th Cir. 2012) (held that exigent circumstances justified a warrantless seizure of the defendant’s computer in a P2P child pornography case, where, during an interview, an investigator informed the defendant of the substance of the investigation, and told him that his computer contained an “identifying marker the police were tracking” and it was it “objectively reasonable to seize a container an officer has probable cause to believe contains evidence of a crime, rather than leave it unguarded in the hands of a suspect.”); *United States v. Diaz*, 435 Fed. Appx. 329, 332 (5th Cir. 2011) (held that exigent circumstances justifying a warrantless seizure of the defendant’s computer where agents had probable cause to believe the computer contained child pornography, and where the defendant denied owning a computer then attempted to conceal the computer he had denied owning.)

was not at home or in possession of the computer. Moreover, there was no evidence of ongoing criminal activity by the defendant. Ms. Nine did not reveal any incriminating information about defendant to agents, nor is there any evidence that had defendant admitted to any wrongdoing. Indeed, defendant never been in contact with agents previously or on that day. The three agents had an open-ended invitation from defendant's roommate to remain in inside the apartment, which they could have done until defendant returned or a warrant was obtained.

While it is possible for electronic data to be deleted remotely, Agent Sale testified that the computer tower was not connected to the internet on the day of the knock and talk. Tr. 103-104. However, Agent Posler later clarified that the computer was connected to the router via an ethernet cable, and that router was connected to the incoming modem. He stated that he disconnected these devices prior to photographing the scene. However, there is no evidence that the defendant was capable of remotely destroying evidence.

Further, agents had ample opportunity to seek a warrant by electronic means under Fed. R. Crim. P. 41(d)(3). The Ninth Circuit has found that government is required "to attempt, in good faith, to secure a warrant or present evidence explaining why a telephone warrant was unavailable or impractical." *Alvarez*, 810 F. 2d at 883. Again, agents had an open-ended invitation to remain at the apartment and keep potential evidence secure. Defendant was not at the residence, and agents had no evidence, other than speculation, to assume defendant would imminently return. Indeed, Agent Sale himself felt that defendant was avoiding

them and had no idea when he might return. Also, while it is true that some of the time spent during the investigation on that day, involved Agent Sale driving to and from defendant's workplace, the seizure occurred at around approximately 12:30 PM on a work day, when the District Court was open for public business.⁹ Agent Sale also felt that he had to time consult with government attorneys prior to the seizure.

The Court recognizes that seeking an electronic warrant is not a simple, instantaneous process, however, "police cannot avoid the good faith requirement of attempting to obtain an arrest warrant because of an imagined delay." *United States v. George*, 883 F.2d 1407, 1415 (9th Cir. 1989) Under these facts, there was no sufficient reason why the government could not have at least attempted to secure such a warrant while awaiting defendant's return.¹⁰ There was no emergency situation or threat that suspected evidence would be imminently destroyed. Agents did speculate that defendant might have returned while waiting for approval from a Magistrate Judge, which would have implicated officer safety concerns if both defendant and Ms. Nine worked together to overcome agents. The Court is sensitive to such concerns, but the government bears a heavy burden in justifying a search or seizure without a warrant. "The [g]overnment does not satisfy this

⁹ Even if the District Court were closed or near to closing for the day, the District of Oregon maintains a rotation of on duty Magistrate and District Judges to handle emergency matters outside of normal business hours.

¹⁰ Cf. *U.S. v. Mickle*, 886 F. 2d 1320 (9th Cir. 1989) (Police officers responding to a reported gunshot entered a residence without warrant to provide assistance when after knocking on door, surveilling the perimeter and speaking with neighbors).

burden by leading a court to speculating about when may or might have been the circumstances surrounding the warrantless search [or seizure].” *United States v. Hoffman*, 607 F.2d 280, 283–84 (9th Cir. 1979) (internal citations omitted). The evidence does not support finding this as an exigency, given that defendant was not on the premises and seemed to be avoiding contact with agents. Ms. Nine cooperated with agents during their investigation, even asking defendant to come speak with agents.

The Government bears the burden to demonstrate that exceptional circumstances justify departing from the warrant requirement. *Spetz*, 721 F. ed. At 1465-66. The Court finds that the government has not met that burden here. The sweep of the government’s exigency argument goes too far beyond what has been found permissible in previous cases. The Court also finds the agents could have secured the area and obtained a telephonic warrant without fear of destruction of the evidence.

Having weighed benefits of deterrence and costs of suppression, the Court GRANTS defendant’s motion to suppress.¹¹

///

///

///

///

¹¹ Having found that the initial seizure of the devices violated the Fourth Amendment, the Court need not examine deeply defendant’s arguments regarding the sufficiency of the subsequent search warrants.

II. *Franks Hearing*

The Court denies defendant's motion for a *Franks* hearing. The Ninth Circuit has identified five requirements which must be met before a defendant is entitled to a *Franks* hearing:

- (1) the defendant must allege specifically which portions of the warrant affidavit are claimed to be false; (2) the defendant must contend that the false statements or omissions were deliberately or recklessly made; (3) a detailed offer of proof, including affidavits, must accompany the allegations; (4) the veracity of only the affiant must be challenged; and (5) the challenged statements must be necessary to find probable cause.

United States v. DiCesare, 765 F.2d 890, 894-95 (9th Cir.), amended, 777 F.2d 543 (1985) (citation omitted). There is "a presumption for validity with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154, 171 (1978).

Defendant raises essentially three *Franks* claims, (1) the warrant lacked probable cause, (2) Agent Sale failed to follow protocol, and (3) Agent Sale did not review the files transferred until a month after Agent Huntoon observed and downloaded them in contrast to statements in his affidavit

First, defendant argues that the warrant lacked probable cause, was dependent on the fruits of an illegal search and seizure, as well as omitted and added material facts in violation of the law and good faith under *Leon*. Defendant also claims that in the affidavit for the search warrant the files were incorrectly described as being known child pornography. In his affidavit, Agent Sale wrote that on September 16, 2012, Agent Huntoon identified a computer at a particular IP

address “that was offering to share at least 52 files of known child pornography.” Ex. A at 58, ¶ 30. In fact, the computer Agent Huntoon identified was offering to share “at least 52 file(s) of investigative interest.” Ex. A at 13; Ex. 1 at 1; Huntoon Decl. ¶ 6. Files of investigative interest are often, but are not always, child pornography. *Id.* at ¶ 5. Agent Sale testified that the affidavit’s probable cause was based off the content of the files downloaded and not the names of the files. Tr. 123. The Court finds, based on Agent Sale’s testimony, the statement was not made deliberately or recklessly in the affidavit.

Defendant also makes repeated references to the fact that NCMEC reported that only one of the downloaded files depicted an identified child, and even then, cautioned that the file may or may not constitute child pornography. The government notes that NCMEC did not review the contents of the downloaded files, so it is not surprising that they could not say whether any of them contained child pornography. Nonetheless, all the files did contain child pornography. Agent Sale looked at each file and described each in detail in the affidavit. Ex. A at 59-60, ¶ 36. Each constitutes child pornography, regardless of whether the children depicted in them have been identified.

Second, defendant also argues that Agent Sale failed to follow Secret Service procedure by logging evidence correctly and in a timely manner. Defendant alleges that Agent Sale received a disc containing the files in question from Agent Huntoon on September 19, 2012, but Agent Sale did not place the disc into evidence until November 27, 2012.

Third, defendant contends that Agent Sale did not review the files transferred until a month after Agent Huntoon observed and downloaded them in contrast to his affidavit. It is true that Agent Sale did not receive the disk in question until September 19, 2012. But his affidavit mentions his knowledge on September 16, 2012 that Agent Huntoon identified a computer that was offering to share at least 52 files of known child pornography. Defendant argues that defendant could not have “known” about the files on September 16, 2012 based on his own report.

The government notes that when Agent Sale is describing the events of September 16 and 17, he was simply describing the information Agent Huntoon provided him. Specifically, he noted in his affidavit that Agent Huntoon was investigating to identify people who were in possession of and sharing child pornography and that Agent Huntoon identified a computer with a particular IP address and downloaded seven complete files from the address.

Defendant arguments do not rise to the standard required for granting a *Franks* motion. There are some minor inconsistencies in the affidavit, but, based on the submissions of the parties and the testimony offered at oral argument, the Court finds that they do not rise to deliberate falsehoods or reckless disregard for the truth.

CONCLUSION

For the reasons set forth herein, defendant Motion to Suppress (Doc. 24) is GRANTED. The request for production of witness statements is denied without

prejudice. Finally, the Court denies the motion for a *Franks* hearing.¹² The parties shall file a joint status report with the Court updating the Court on their positions moving forward, including whether an appeal of this ruling will be sought within 21 days of this order.

IT IS SO ORDERED.

DATED THIS 30th day of December, 2020

/s/Ann Aiken

ANN AIKEN

U.S. DISTRICT JUDGE

¹² The Court also denies Defendant's Motion for Reconsideration. Doc. 40.